Redes privadas virtuales VPN

Tema 3 SAD

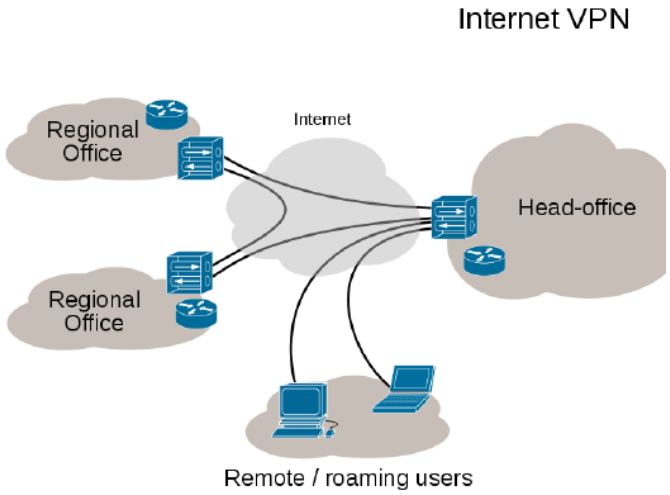
Vicente Sánchez Patón

I.E.S Gregorio Prieto

Beneficios y desventajas con respecto a las líneas dedicadas

En años pasados si una oficina remota necesitaba conectarse a una computadora central o red en las oficinas principales de la compañía significaba arrendar líneas dedicadas entre las ubicaciones. Estas líneas dedicadas arrendadas proveen relativamente rápidas y seguras comunicaciones entre los sitios, pero son muy costosas.

Para adecuar usuarios móviles las compañías tendrían que configurar marcado (dial-in) dedicado de Servidores de Acceso Remoto (RAS = Remote Access Servers). El RAS tendrá un modem, o varios modems, y la compañía debería tener una línea telefónica corriendo para cada modem. Los usuario móviles pueden conectarse a una red de este modo, pero la velocidad será dolorosamente lenta y dificulta hace mucho trabajo productivo.



Beneficios y desventajas con respecto a las líneas dedicadas

Con el advenimiento del Internet mucho de esto ha cambiado. Si una red de servidores y conexiones de red (valga la redundancia) interconecta computadoras alrededor del globo, entonces por que debería una compañía gastar dinero y crear dolores de cabeza administrativos para implementar líneas dedicadas arrendadas y bancos de modems de marcado (dial-in). Por que no solamente usar Internet?

Bien, el primer reto es que tu necesitas ser capaz de escoger "quien" tiene que ver "que" información. Si tu simplemente abres la red completa al Internet sería virtualmente imposible implementar un medio eficaz para cuidar que usuarios no autorizados ganen acceso a la red corporativa. Compañías gastan toneladas de dinero para montar cortafuegos (Firewalls) y otras medidas de seguridad dirigidas específicamente para asegurarse que nadie desde el Internet público pueda entrar en la red interna.

¿Cómo reconciliar el deficiente bloqueo de Internet para acceder a la red interna con las deficiencias de tus usuarios remotos para conectarse a la red interna? Tu implementas una Red Privada Virtual (VPN = Virtual Private Network). Una VPN crea un tunel virtual conectando dos terminales. El tráfico dentro del tunel VPN está encriptado, así que otros usuarios de la red pública de Internet no pueden fácilmente mirar comunicaciones interceptadas.

Beneficios y desventajas con respecto a las líneas dedicadas

Implementando una VPN, una compañía puede proveer acceso a la red interna privada a clientes alrededor del mundo en cualquier ubicación con acceso al Internet público. Esto elimina los dolores de cabeza financieros y administrativos asociados con una tradicional línea arrendada de red de área amplia (WAN = Wide Area Network) y permite a usuarios móviles y remotos ser más productivos. Lo mejor de todo si está bien implementado, lo hace sin impacto a la seguridad e integridad de los sistemas de cómputo y datos en la red privada de la compañía.

VPN´s tradicionales se basan en IPSec (Internet Protocol Security) para construir un tunel entre dos terminales. IPSec trabaja sobre la capa de red (Network layer) en el modelo OSI – asegurando todos los datos que viajan, a través, de dos terminales sin una asociación con alguna aplicación específica. Cuando se conectan sobre una VPN IPSec la computadora cliente es virtualmente un miembro pleno de la red corporativa – capaz de ver y potencialmente acceder a la red completa.

Beneficios y desventajas con respecto a las líneas dedicadas

Si una organización necesita conectividad más allá de los límites físicos de su central, implantar una VPN puede ser una buena solución con importantes ventajas:

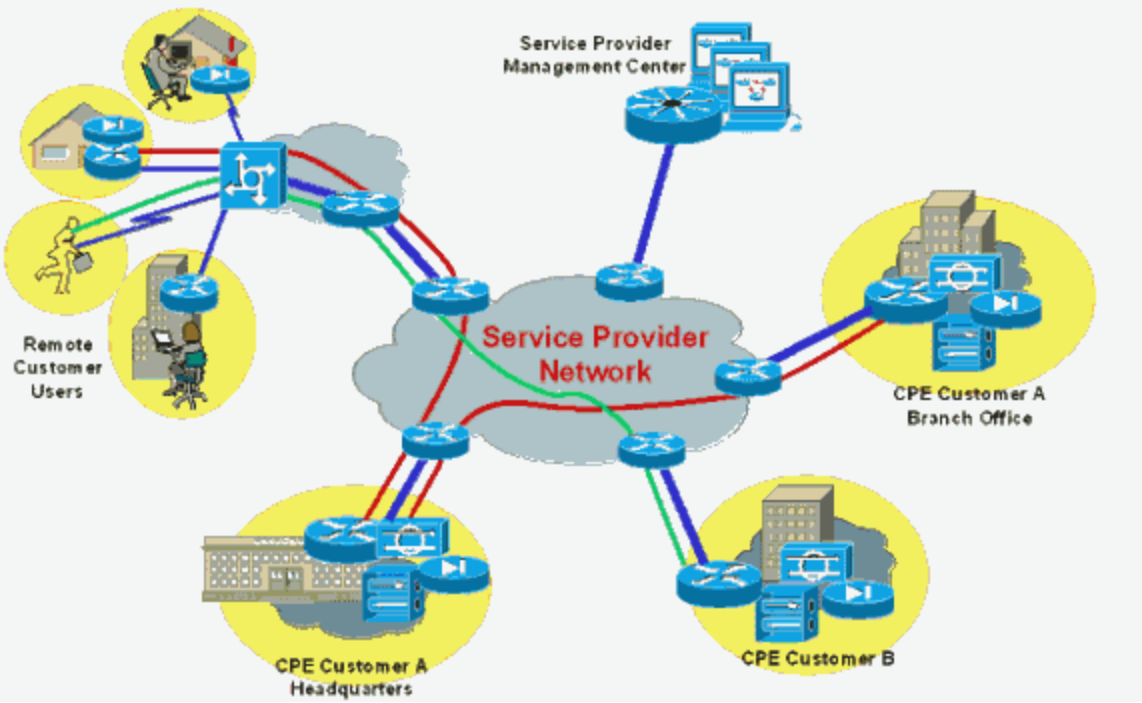
Ventajas

- Una de las ventajas más significativas es el hecho de que las VPN permiten la integridad, confidencialidad y seguridad de los datos.
- Reducción de costes, frente a líneas dedicadas.
- Sencilla de usar, una vez conectados a la VPN, se trabaja como si fuera una LAN.
- Control de Acceso basado en políticas de la organización
- Herramientas de diagnóstico remoto.
- Los algoritmos de compresión optimizan el tráfico del cliente.

Beneficios y desventajas con respecto a las líneas dedicadas

Desventajas

El uso de redes VPN no tiene apenas desventajas, sin embargo cabe señalar que como toda la información se envía a través de Internet, es necesario tener una buena conexión. Con una conexión a Internet más básica, se pueden experimentar problemas y lentitud.



Tipo de conexión VPN

Una red privada virtual, RPV, o VPN de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

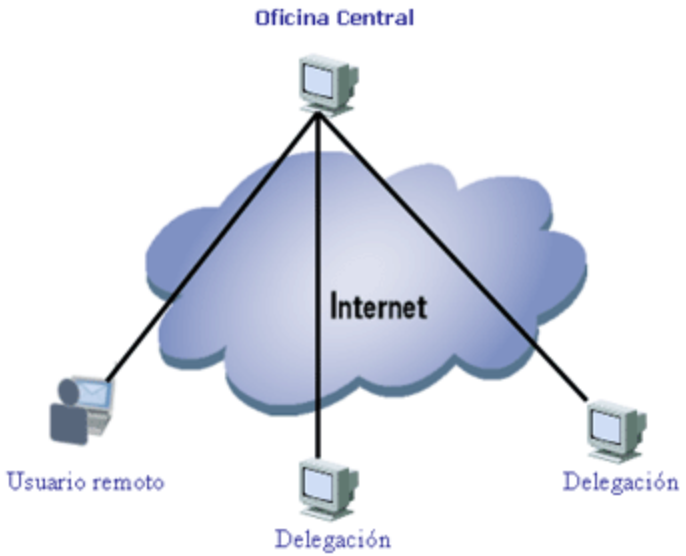
Ejemplos comunes son la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

Básicamente existen tres arquitecturas de conexión VPN:

- VPN acceso remoto
- VPN de sitio a sitio
- VPN sobre LAN

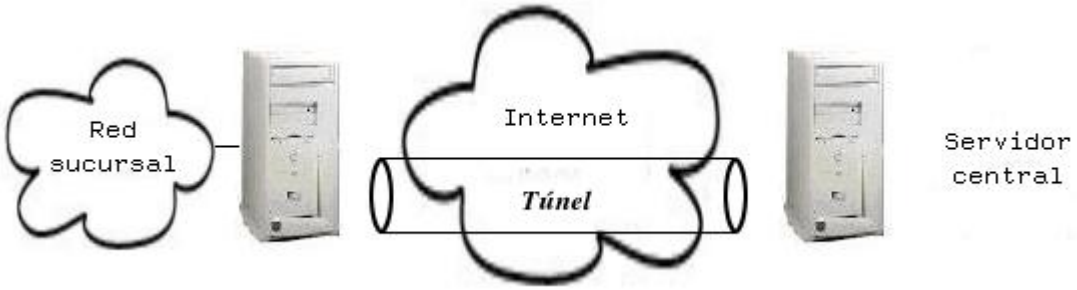
VPN de acceso remoto

Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).



VPN de sitio a sitio o punto a punto (tunneling)

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a puntos tradicionales (realizados comúnmente mediante conexiones de cable físicas entre los nodos), sobre todo en las comunicaciones internacionales. Es más común el siguiente punto, también llamado tecnología de túnel o tunneling.



VPN de sitio a sitio o punto a punto (tunneling)

La técnica de tunneling consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras. El establecimiento de dicho túnel se implementa incluyendo un PDU determinada dentro de otra PDU con el objetivo de transmitirla desde un extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la PDU encapsulada. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes. El túnel queda definido por los puntos extremos y el protocolo de comunicación empleado, que entre otros, podría ser SSH.

VPN sobre LAN

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WIFI).

Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal de recursos humanos habilitado pueda acceder a la información.

Tipos de conexión VPN

Conexión de acceso remoto

Una conexión de acceso remoto es realizada por un cliente o un usuario de una computadora que se conecta a una red privada, los paquetes enviados a través de la conexión VPN son originados al cliente de acceso remoto, y éste se autentifica al servidor de acceso remoto, y el servidor se autentifica ante el cliente.

Conexión VPN router a router

Una conexión VPN router a router es realizada por un router, y este a su vez se conecta a una red privada. En este tipo de conexión, los paquetes enviados desde cualquier router no se originan en los routers. El router que realiza la llamada se autentifica ante el router que responde y este a su vez se autentica ante el router que realiza la llamada y también sirve para la intranet.

Conexión VPN firewall a firewall

Una conexión VPN firewall a firewall es realizada por uno de ellos, y éste a su vez se conecta a una red privada. En este tipo de conexión, los paquetes son enviados desde cualquier usuario en Internet. El firewall que realiza la llamada se autentifica ante el que responde y éste a su vez se autentifica ante el llamante.

Protocolos que generan una VPN: PPTP, L2F, L2TP.

Protocolos de túnel

Los principales protocolos de túnel son:

- PPTP (Protocolo de túnel punto a punto) es un protocolo de capa 2 desarrollado por Microsoft, 3Com, Ascend, US Robotics y ECI Telematics.
- L2F (Reenvío de capa dos) es un protocolo de capa 2 desarrollado por Cisco, Northern Telecom y Shiva. Actualmente es casi obsoleto.
- L2TP (Protocolo de túnel de capa dos), el resultado del trabajo del IETF (RFC 2661), incluye todas las características de PPTP y L2F. Es un protocolo de capa 2 basado en PPP.
- IPSec es un protocolo de capa 3 creado por el IETF que puede enviar datos cifrados para redes IP.

Protocolos que generan una VPN: PPTP, L2F, L2TP.

Protocolo PPTP

El principio del PPTP (*Protocolo de túnel punto a punto) consiste en crear tramas con el protocolo PPP y encapsularlas mediante un datagrama de IP.*

Por lo tanto, con este tipo de conexión, los equipos remotos en dos redes de área local se conectan con una conexión de igual a igual (con un sistema de autenticación/cifrado) y el paquete se envía dentro de un datagrama de IP.

De esta manera, los datos de la red de área local (así como las direcciones de los equipos que se encuentran en el encabezado del mensaje) se encapsulan dentro de un mensaje PPP, que a su vez está encapsulado dentro de un mensaje IP.

Protocolos que generan una VPN: PPTP, L2F, L2TP.

Protocolo L2F

El protocolo L2F (Layer 2 Forwarding) se creó en las primeras etapas del desarrollo de la red privada virtual. Como PPTP, L2F fue diseñado por Cisco para establecer túneles de tráfico desde usuarios remotos hasta sus sedes corporativas. La principal diferencia entre PPTP y L2F es que, como el establecimiento de túneles de L2F no depende del protocolo IP (Internet Protocol), es capaz de trabajar directamente con otros medios, como Frame Relay o ATM. Como PPTP, L2F utiliza el protocolo PPP para la autenticación del usuario remoto, pero también implementa otros sistemas de autenticación como TACACS+ (Terminal Access Controller Access Control System) y RADIUS (Remote Authentication Dial-In User Service). L2F también difiere de PPTP en que permite que los túneles contengan más de una conexión.

Hay dos niveles de autenticación del usuario, primero por parte del ISP (proveedor de servicio de red), anterior al establecimiento del túnel, y posteriormente, cuando se ha establecido la conexión con la pasarela corporativa. Como L2F es un protocolo de Nivel de enlace de datos según el Modelo de Referencia OSI, ofrece a los usuarios la misma flexibilidad que PPTP para manejar protocolos distintos a IP, como IPX o NetBEUI.

Protocolos que generan una VPN: PPTP, L2F, L2TP.

Protocolo L2TP

L2TP es un protocolo de túnel estándar (estandarizado en una RFC, solicitud de comentarios) muy similar al PPTP. L2TP encapsula tramas PPP, que a su vez encapsulan otros protocolos (como IP, IPX o NetBIOS).